Republic of the Philippines
DON HONORIO VENTURA STATE UNIVERSITY

Cabambangan, Bacolor, Pampanga

COLLEGE OF COMPUTING STUDIES

(6345) 458 0021 Local 211

Email: ccs@dhvsu.edu.ph

http://dhvsu.edu.ph

INFORMATION TECHNOLOGY DEPARTMENT

MIDTERM – CASE STUDY

Case Study Activity: The SolarWinds Hack – A Lesson in Information Security Management Strategies and Governance

Objective:

This case study activity is designed to help students critically analyze the **SolarWinds hack**, understand its implications, and relate it to key concepts in Information Security Management Strategies and Governance. By completing this activity, students will explore how governance frameworks, incident response strategies, and risk management practices could have mitigated or prevented the attack.

Instructions:

Research and review credible sources or articles that discuss the SolarWinds hack (You may use journal articles, online resources, or assigned reading materials).

Focus on understanding:

- How the attack was carried out (methods and tactics).

Isinagawa ang atake sa pamamagitan ng paggamit ng supply chain attack, na kung saan ang supply chain attack na ito ay nagtatarget sa mga third-party vendors ng software at hardware ng isang kumpanya. Sa halip na diretang i-hack ang kumpanya o network, ang kanilang produkto ang kanilang tinatarget. Sa nangyari sa SolarWinds, ang Orion software ang kanilang hinack at nag insert ng malicious code sa update ng Orion software. Itong trojanized na update ay pinadala sa mga customer ng SolarWinds ng walang kalam-alam na ito'y compromised.
Sa sandaling ma install ang update sa mga sistema ng customer, nagkakaroon ng backdoor access ang mga attackers. Na kung saan dito nagkakaroon sila ng kakayahan at makontrol at makakuha ng impormasyon.

Sa pamamagitan ng alert system, nagkaroon ang mga attackers ng kakayahang mamonitor at makontrol ang paglabas ng mga updates, na nagbigay-daan para sa kanilang malware na makalusot sa mga system ng SolarWinds at sa kanilang mga kustomer.
Ang SolarWinds ay isang perpektong target para sa ganitong uri ng supply chain attack dahil ang kanilang Orion software ay ginagamit ng maraming multinational companies at ahensya ng gobyerno; ang tanging kailangan ng mga hacker ay mag-install ng malicious code sa isang bagong batch ng software na ipinamamahagi ng SolarWinds bilang update o patch.

- The role of the supply chain in the vulnerability.

Ang supply chain ay may mahalagang papel sa kahinaan ng SolarWinds dahil:

- Ang mga kumpanya, kabilang ang SolarWinds, ay madalas na umaasa sa mga third-party vendors para sa kanilang software at hardware; kapag ang mga third-party na ito ay nagiging target ng mga attacker, nagiging daan ito upang ma-access ang mga network ng mga kliyente.
- Sa kaso ng SolarWinds, nagkaroon ng pagkakataon ang mga attacker na mag-insert ng malicious code sa mga legitimate updates ng kanilang Orion software, kaya't ang mga gumagamit ay hindi nagiging mapaghinala at nag-i-install ng compromised na software nang hindi nalalaman.
- Maraming kumpanya ang hindi sapat ang pagtuon sa seguridad ng kanilang mga third-party vendors, na nagiging sanhi ng mga kahinaan na maaaring ma-exploit ng mga attacker; sa SolarWinds, ang kakulangan ng pagsuri at oversight sa kanilang supply chain ay nagbigay-daan sa malawakang breach na nagdulot ng malaking pinsala sa kanilang mga kliyente.

Ang supply chain ay ang buong proseso ng paggawa at paghahatid ng produkto mula sa simula hanggang sa makuha ito ng mga tao.

- The consequences for organizations and industries affected.

Sa nangyaring pag-atake sa SolarWinds, maraming tao ang naapektuhan, kabilang ang mga empleyado, private sectors, at ilang government agencies tulad ng Department of Homeland Security, State Department, at Department of Energy. Ang mga kompanyang apektado ay kinabibilangan ng SolarWinds, Microsoft, Cisco, Intel, at Deloitte. Dahil sa nangyaring ito, ito ang naging kahinatnan ng nangyari:

- Isa sa mga consequences na hinarap ng SolarWinds sa pag-atake sa kanilang organization ay ang financial loss, kasama na rito ang pagbabayad para sa pag-iimbestiga, remediation ng breach, at pagtaas ng mga hakbang sa seguridad. Bukod dito, ang mga kumpanya na naapektuhan at naharap din sa potensyal na legal liabilities at reputational damage, na nagdulot ng kawalan ng tiwala mula sa kanilang kliyente at partners. Ayon pa sa study na binigay, umabot ng $100 billion dollars ang nagastos ng private sector dito habang ang SolarWind ay nagasto ng $18 -$19 million Hindi pa kasama dito ang gastos ng mga karagdagang panukalang seguridad at software, pagtaas ng pondo para sa mga bagong pagsasanay sa cyber para sa mga empleyado, at kabayaran para sa mga nakaramdam na lubos silang naapektuhan ng pag-atake na ito.
- Dagdag pa rito, ang pagkawala ng tiwala ng mga customers at stakeholders dahil ang kanilang sensitive data at personal information ay nakompromiso.
- Dahil dito, nahirapan ang mga organisasyon na maibalik ang kumpiyansa ng kanilang mga kliyente, na nagresulta sa pagbaba ng benta at posibleng pagkawala ng mga kasosyo sa negosyo. Ang mga kumpanya ay pinilit din na mamuhunan ng mas malaki sa cybersecurity measures upang maiwasan ang mga ganitong insidente sa hinaharap.
- Ang mga epekto ng pag-atake ay hindi lamang limitado sa pananalapi, kundi pati na rin sa operasyon ng mga kumpanya. Kinailangan nilang baguhin ang kanilang mga sistema at proseso, na nagdulot ng pagkaantala sa kanilang mga proyekto at serbisyo.

- How the incident was discovered and addressed.

Nadiskubre ng FireEye, isang cybersecurity company sa California, na ang kanilang systems ay nakompromiso noong Disyembre 2020. Sa kanilang imbestigasyon, nalaman nilang nagmula ang pag-atake sa SolarWinds Orion software. Sa sunod-sunod na imbestigasyon, natuklasan nila na ang atake ay nangyari sa loob ng ilang buwan. Nalaman din na ang mga hacker ay nakapasok na sa mga systems ng SolarWinds noong Oktubre 2019, bilang isang test run bago ang kanilang pangunahing atake noong Marso 2020.

Pagkatapos madiskubre ang pag-atake, naglabas ang administrasyon ni Biden ng pahayag tungkol sa isang executive order na nagtatakda ng ilang parusa laban sa Russia. Bukod sa mga parusang ito, opisyal na inakusahan ng White House ang SVR ng Russia, kasama ang mga grupong APT 29, Cozy Bear, at Dukes, bilang mga salarin sa atakeng ito.

Relate the Incident to Information Security Management Strategies:

Analyze the incident in relation to the following security management components:

- **Risk Management:** How did the attack expose failures in risk management? Could stronger risk assessments have prevented it?

Ang pag-atake sa SolarWinds ay nagbigay-diin sa mga pagkukulang sa risk management kabilang na ang:

1. Kakulangan ng Pagsusuri sa mga Third-party vendors. Maraming mga kumpanya ang umaasa sa third-party vendors nang hindi nagsasagawa ng masusing pagsusuri, na nagbibigay-daan para sa mga attacker na mag-inject ng malicious code sa mga update. Kung may malakas na risk-assessment na pinapatupad, mas mataas ang tyansa na ma -prevent ang ganitong insidente dahil makikilala at makikita ang mga potensyal na pangani at maiiwasan ang mga kahinaan sa seguridad.
2. Kakulangan sa regular na pagsusuri at monitoring na nagbigay dan sa mga attacker na hindi mapansin. Kung masusing minomonior at chinecheck ang kanilang system, maari nilang ma-detect kaagad ang mga kahinaan at maiwasan ang pagkalat ng atake.
3. Kakulangan sa pagsasanay ng mga empleyado at hindi sapat na kaalaman tungkol sa cybersecurity. Kung ang mge empleyado ay may mas mahusay na pagsasanay at kaalaman, maharani nilang mas madaling makilala ang mga potensyal nab anta at maiwasan ang mga pagkakamali na naging sanhi ng pag-atake.
4. Ang Hindi Pagiging Handa sa mga Advanced Threats**: Maraming organisasyon ang hindi handa sa mga sopistikadong atake tulad ng supply chain attacks. Kung mas mahusay ang kanilang risk management strategies at may mga contingency plans, maaaring na-identify at na-handa sila para sa mga ganitong banta. Ang kakulangan sa paghahanda ay nagresulta sa mas malaking pinsala at mas mahirap na recovery matapos ang insidente.

- **Incident Response Planning:** Assess the effectiveness of the incident response. How could a proactive response plan have limited the damage?

Sa SolarWinds na pag-atake, ang epektibong incident response ay mahalaga. Ang isang proactive response plan ay maaaring nagbigay ng mga hakbang para sa mas maagang pagtukoy at pag-alis sa mga banta, tulad ng mas regular na pagsusuri sa mga sistema at mas mahigpit na kontrol sa access. Kung may mga detalyadong protocols at training para sa mga tauhan, maaaring nabawasan ang saklaw ng pinsala at mas mabilis na na-recover ang mga naapektuhang system.

Sa SolarWinds na pag-atake, ang kakulangan sa proactive response planning ay nagresulta sa malawakang pinsala at pagnanakaw ng impormasyon. Sa mga ganitong sitwasyon, mahalagang magkaroon ng mga sumusunod na hakbang:

1. **Pagsusuri at Pagsubok**: Ang regular na pagsusuri sa mga network at application ay makakatulong upang matukoy ang mga kahinaan bago pa man magamit ng mga attacker.

2. **Pag-monitor ng Aktibidad**: Ang mas mahigpit na pag-monitor ng anomalya sa network ay maaaring makakita ng mga hindi pangkaraniwang aktibidad na maaaring magpahiwatig ng pag-atake.

3. **Pagsasanay ng mga Empleyado**: Ang pagtutok sa cybersecurity awareness training ay mahalaga upang maging handa ang mga empleyado sa mga phishing at iba pang uri ng social engineering attacks.

4. **Incident Response Team**: Ang pagkakaroon ng dedikadong team na handang tumugon sa mga insidente ay nakakatulong sa mabilis na pag-responde at pag-recover.

5. **Regular na Update at Patch Management**: Ang pagkakaroon ng sistematikong proseso para sa pag-update ng software at pag-patch ng vulnerabilities ay makakatulong upang maiwasan ang paggamit ng mga kilalang kahinaan.

Sa pamamagitan ng mga hakbang na ito, ang epekto ng SolarWinds na pag-atake ay maaaring nabawasan, at mas mabilis na naayos ang mga naapektuhang sistema. Ang proactive na plano ay hindi lamang nakakatulong sa pagtugon sa mga insidente kundi nagbibigay din ng mas malaking tiwala sa seguridad ng buong organisasyon.

Explore Information Security Governance:

• **Evaluate the governance structures** that failed in this case.

Sa kaso ng SolarWinds attack, ilang aspeto ng governance structures ang nagtagumpay na magpahina sa seguridad.

1. **Kakulangan sa Pagsusuri sa Third-Party Vendors**: Ang kumpanya ay hindi sapat na nag-assess ng security measures ng kanilang mga third-party vendors. Dapat ay may mas mahigpit na pagsusuri at monitoring sa mga partner na ito.

2. **Limitadong Incident Response Plans**: Ang mga plano para sa pagtugon sa insidente ay hindi sapat na naipapatupad. Dapat ay may mas malinaw at mabilis na proseso para sa pagtukoy at pagtugon sa mga banta.

3. **Mahinang Access Controls**: Ang pamamahala sa access sa sensitive data at systems ay hindi naging mahigpit. Kailangan ay may mas mahusay na control at authentication measures upang maiwasan ang unauthorized access.

4. **Kakulangan sa Transparency at Reporting**: Ang kakulangan sa bukas na komunikasyon at reporting sa mga security risks at vulnerabilities ay nagpalala sa sitwasyon. Dapat ay may mas sistematikong approach sa pag-uulat ng mga problema sa seguridad.

5. **Hindi Pagsunod sa Best Practices**: Maraming kumpanya ang hindi sumunod sa mga industry standards at best practices sa cybersecurity, na nagbigay daan sa pag-atake.

Ang mga aspetong ito ay nagpapakita na ang mga governance structures ay hindi naging epektibo sa pagprotekta laban sa mga sophisticated cyber threats gaya ng SolarWinds attack.

Discuss Defense in Depth Strategy:

• Consider how a **defense in depth** approach could have provided more layers of protection against the SolarWinds hack.

Ang "defense in depth" ay isang diskarte sa seguridad na gumagamit ng maraming layer ng proteksyon upang mapigilan ang mga banta at atake. Sa halip na umasa lamang sa isang solong sistema o tool, ang diskarte ito ay nagsasama ng iba’t ibang uri ng seguridad, tulad ng:

1. **Physical Security**: Mga pisikal na hakbang tulad ng mga lock, CCTV, at security personnel.

2. **Network Security**: Firewalls, intrusion detection systems, at segmentasyon ng network.

3. **Endpoint Security**: Antivirus software at pag-update ng mga device para sa proteksyon laban sa malware.

4. **Application Security**: Secure coding practices at regular na pagsusuri sa mga application.

5. **User Awareness Training**: Pagsasanay para sa mga empleyado ukol sa mga panganib sa seguridad, phishing, at tamang paggamit ng mga system.

Sa ganitong paraan, kahit na may magtagumpay na atake sa isang layer, may iba pang mga layer na makakapagbigay ng proteksyon.

Narito ang karagdagang mga paraan kung paano ang "defense in depth" ay maaaring nagbigay ng mas maraming layer ng proteksyon laban sa SolarWinds hack:

6. **Application Whitelisting**: Ang pagpapatupad ng application whitelisting ay magpapahintulot lamang sa mga kilalang at pinagkakatiwalaang application na tumakbo. Ito ay makakapigil sa mga hindi awtorisadong software, tulad ng malware, na makapasok sa sistema.

7. **Data Encryption**: Ang pag-encrypt ng sensitibong data, kapwa sa pahinga at sa transit, ay makakatulong na protektahan ito mula sa pag-access ng mga hindi awtorisadong tao, kahit na makuha nila ang data.

8. **Incident Response Plan**: Ang pagkakaroon ng maayos na plano sa pagtugon sa insidente ay mahalaga. Ang mga kumpanya ay dapat handa na kumilos agad sa oras ng breach, kasama ang mga protocol para sa pagkilala, pagsugpo, at pag-uulat ng insidente.

9. **Regular na Training at Awareness Programs**: Ang patuloy na pagsasanay para sa mga empleyado tungkol sa cybersecurity risks, phishing attacks, at tamang pag-uugali sa online ay makakatulong na mabawasan ang panganib ng human error, na madalas na nagiging sanhi ng breaches.

10. **Third-Party Risk Management**: Ang pagsusuri at pag-monitor sa mga third-party vendors at partners ay mahalaga, lalo na kung sila ay may access sa mga sensitibong sistema. Ang masusing due diligence ay makakatulong na matiyak na ang kanilang seguridad ay naaayon sa mga pamantayan ng kumpanya.

Sa pamamagitan ng pagsasama-sama ng mga hakbang na ito, ang "defense in depth" ay makakapagbigay ng mas kumpleto at matibay na proteksyon laban sa mga sophisticated na atake tulad ng SolarWinds hack.

• Explore whether a **Zero Trust** security model would have been more effective in mitigating the attack.

Ang Zero Trust security model ay naglalayong pigilan ang mga atake sa pamamagitan ng pag-aakalang walang sinuman, kahit na ang mga nasa loob ng network, ay maaasahan. Narito kung paano ito maaaring naging mas epektibo sa pagpapababa ng panganib ng SolarWinds hack:

1. **Walang Awtorisadong Access**: Sa Zero Trust, lahat ng access ay kailangang i-verify bago pahintulutan, kahit na ang mga internal na gumagamit. Kung ang modelo ay naipatupad, ang mga attacker na nakapasok sa network ay hindi agad makaka-access sa mga sensitibong sistema.

2. **Patuloy na Pagsusuri**: Ang Zero Trust ay nagtataguyod ng patuloy na pagsusuri ng mga access at aktibidad. Sa ganitong paraan, ang anumang pagbabago sa behavior ng user o anomalya ay agad na matutukoy, na nag-aalerto sa mga admin sa posibleng breach.

3. **Principle of Least Privilege**: Ang Zero Trust ay nagtataguyod ng pagbibigay ng pinakamababang pribilehiyo sa mga user. Sa SolarWinds case, kung ang mga user ay may limitadong access lamang, mababawasan ang epekto ng pag-atake.

4. **Segmentation**: Ang pag-segment ng network sa mas maliliit na bahagi ay makakatulong na mapigilan ang pagkalat ng malware. Sa ilalim ng Zero Trust, ang bawat bahagi ng network ay may sariling seguridad at authentication, kaya kahit na ma-access ng attacker ang isang bahagi, hindi ito madaling makakaapekto sa iba pang bahagi.

5. **Multi-Factor Authentication (MFA)**: Ang pagkakaroon ng MFA bilang bahagi ng Zero Trust ay nagdaragdag ng layer ng proteksyon, na nagpapahirap sa mga attacker na makapasok kahit na nakuha nila ang mga credentials.

Sa kabuuan, kung ang Zero Trust security model ay naipatupad bago ang SolarWinds hack, maaaring naging mas mahirap para sa mga attacker na makapasok at makapagpatuloy sa kanilang atake, na nagbigay ng mas mataas na antas ng proteksyon para sa mga kritikal na sistema.

Prepare for a Class Discussion:

• Be ready to present your findings in class. You will discuss your understanding of the incident and how information security management strategies can be applied to avoid similar incidents in the future.

Important notes:

- Ayon sa isang ulat mula sa Director of National Intelligence, ang pangunahing target ng Russia ay kritikal na imprastruktura, supply chains, at maraming aspeto na itinuturing na kritikal sa e konomiya ng isang bansa. Sa pamamagitan ng pag-
  atake sa mga bagay na ito, nagagawa ng Russia na pahinain ang ekonomiya, paraan ng pamum uhay, at mga operasyon na mahalaga sa pagpapanatili ng seguridad at katahimikan sa isang est ado.

Other questions

Bakit hindi napansin ng SolarWinds na nahack sila?

Hindi kaagad napansin ng SolarWinds na sila ay na-hack dahil sa ilang pangunahing dahilan: una, ang Sunburst malware ay idinisenyo nang sopistikado, na nagbigay-daan sa mga attacker na magsimula ng kanilang operasyon nang hindi napapansin; pangalawa, gumamit sila ng maraming server na nakabase sa U.S. at nagmimik ng lehitimong network traffic, na nagpapahirap sa pagtukoy ng mga threat detection techniques ng SolarWinds; at pangatlo, ang mahaba nilang dwell time na umabot ng higit sa isang taon ay nagbigay sa kanila ng sapat na panahon upang makapagtipon ng sensitibong impormasyon at makapagsagawa ng mas malawak na operasyon sa loob ng network.

Facts

- SolarWinds ay isang malaking software company na naka-base sa Tulsa, Oklahoma, na nagbibigay ng mga sistema ng pamamahala para sa network at infrastructure monitoring, at iba pang teknikal na serbisyo sa daan-daang libong mga organisasyon sa buong mundo. Isa sa mga produkto ng kumpanya ay ang IT performance monitoring system na tinatawag na Orion.

- Bilang isang IT monitoring system, ang SolarWinds Orion ay may pribilehiyong access sa mga IT system upang makakuha ng log at system performance data. Ang pribilehiyong posisyon at malawakang deployment nito ang naging dahilan kaya naging target ng mga pag-atake ang SolarWinds

- SolarWinds ay ang kumpanya na lumikha ng Orion system. Orion ay isa sa mga pangunahing produkto ng SolarWinds. Ito ay isang IT performance monitoring system na ginagamit ng maraming kumpanya at mga ahensya ng gobyerno upang masubaybayan at pamahalaan ang kanilang mga network at infrastructure. Kaya ang relasyon ng SolarWinds sa Orion ay tulad ng relasyon ng isang manufacturer sa kanyang produkto. Ang SolarWinds ang nagpo-produce, nagbebenta, at nagbibigay ng update sa Orion system. Ang Orion system naman ang ginagamit ng mga kliyente ng SolarWinds para masiguro ang maayos na operasyon ng kanilang IT infrastructure.

Questions:

1. Bakit Napili ng Russia's Foreign Intelligence Service and SolarWinds?
   Ang SolarWinds ay napili ng Russia dahil ito ay isang malaking software na ginagamit ng maraming mga kumpanya at gobyerno upang mapanatili ang kanilang mga sistema at network1. Ang pag-
   atake sa SolarWinds ay naglalaman ng isang "backdoor" na pinaglalagay sa software update na ginag amit ng mga kliyente1. Sa pamamagitan nito, ang mga hackers ay nakakapinsala sa mga sistema ng mga kliyente na gumagamit ng SolarWinds.

2.

Sa mga nakaraang taon, ang bilang ng mga cyber-attacks at mga insidente ay tumaas nang husto. Sa isang mundo na patuloy na nagiging mas digital, ang cybersecurity ay lalong nagiging mahalaga upang masiguro ang kaligtasan ng sensitibong impormasyon at mga tao. Ang papel na ito ay naglalayong ilahad ang layunin pati na rin ang pangkalahatang ideya ng mga cyber at espiya na dibisyon ng Russia. Gayunpaman, ang papel na ito ay hindi naglalayong ilahad ang bawat cyber event na isinagawa ng Russia, kundi aspirasyong saklawin ang isang insidente, ang SolarWinds cyber-attack ng 2020, at ang mga naging epekto nito. Ang SolarWinds attack ay isang malaking cyber-attack na isinagawa ng Foreign Intelligence Service (SVR) ng Russia. Matapos na hindi mapansin ng ilang buwan, nagawa ng Russia na makakuha ng mahalagang intel mula sa ilang pinaka-secure na departamento ng Estados Unidos. Ang papel na ito ay magsisilbing gabay sa pag-atake na ito pati na rin ilarawan ang mga layunin ng Russia sa pagsasagawa ng ganitong mga pag-atake.

Matagal nang kalaban ng Estados Unidos ang Russia. Sa paglago ng kanilang mga dibisyon sa espiya at cyber, lalo pang naging panganib ang Russia sa seguridad at operasyon ng Estados Unidos. Ayon sa isang ulat mula sa Director of National Intelligence, ang pangunahing target ng Russia ay kritikal na imprastruktura, supply chains, at maraming aspeto na itinuturing na kritikal sa ekonomiya ng isang bansa. Sa pamamagitan ng pag-atake sa mga bagay na ito, nagagawa ng Russia na pahinain ang ekonomiya, paraan ng pamumuhay, at mga operasyon na mahalaga sa pagpapanatili ng seguridad at katahimikan sa isang estado.

Bagama't gumagamit ang Russia ng normal na pangangalap ng impormasyon at mga espiya sa lugar, mas nagre-rely sila sa cyber-attacks dahil sa ilang kadahilanan. Una, mas mabilis makapasok sa isang network sa pamamagitan ng digital na paraan kaysa sa paglikha ng takip at pangangalap ng impormasyon nang personal o para sa kawalan ng mas magandang termino, "paglalakad sa harap ng pintuan". Pangalawa, mas mura ang paggamit ng iba't ibang pamamaraan ng pag-hack kaysa magpadala ng ahente sa ibang bansa at bigyan sila ng

mga kinakailangang mapagkukunan para sa kanilang misyon. Ang mga cyber-attacks ay maaaring isagawa sa loob lamang ng ilang minuto kung tama ang pagkakagawa at ang kailangan lang ng isang tao ay isang computer at internet. Bagama't ang mga hacker ng Russia ay napakahusay at sanay sa digital warfare, ang konsepto ay pareho pa rin. At ang huling dahilan kung bakit malakas ang paggamit ng Russia sa cyber-attacks ay dahil madali itong itanggi. Kung ang isang ahente ay mahuling sinusubukang pumasok sa isang organisasyon, madali silang matutunton pabalik sa bansang pinagmulan nila. Gayunpaman, ang isang hacker ay maaaring magpalipat-lipat ng kanilang lokasyon sa maraming bansa, na nagpapahirap sa Estados Unidos o sinumang iba pa na matukoy ang kanilang pinagmulan. At kung mahuli sila, madaling itanggi ng Russia ang anumang kaugnayan sa kanila.

Hacker Groups and Methods

Ang Russia ay nakakagawa ng matagumpay at malayang mga operasyon dahil sa maraming state-sanctioned hacker groups tulad ng APT 29, Fancy Bear, Cozy Bear, at ang Dukes. May iba pang mga hacker groups na, bagamat hindi opisyal na kinikilala ng estado, ay patuloy na pinapayagan na mag-operate sa teritoryo ng Russia basta't nakakabenepisyo sila sa bansa.

Ang mga hacker na ito ay nagta-target sa gobyerno ng Estados Unidos at sa pribadong sektor upang makakuha ng mahalagang impormasyon na magagamit sa mga layuning pampolitika ng Russia. Nais din nilang matuklasan ang mga limitasyon at kahinaan upang mapagsamantalahan ang mga ito para sa karagdagang access sa supply chain ng Estados Unidos.

Bagamat ang mga state-sanctioned hacker groups ng Russia, tulad ng Cozy Bear, Fancy Bear, at ang SVR, ang itinuturong responsable sa SolarWinds attack noong 2020, marami pa ring mga state-tolerated hacker groups ang responsable sa mga mas kamakailang pag-atake tulad ng Continental Pipeline hack at JBS Meatpacking hack. Ang mga hacker na ito ay hindi opisyal na sinusuportahan ng Russia, ngunit kinikilala ang kanilang pag-iral at pinapayagan na mag-operate sa loob ng kanilang teritoryo. Sa ganitong paraan, maikakaila ng Russia ang anumang responsibilidad sa mga cyber-attacks na ginagawa ng mga grupong ito, ngunit mayroon pa rin silang mutual na relasyon.

Ang mga grupong ito ay pangunahing nakatuon sa maliliit na ransomware attacks para sa pera at cryptocurrencies sa halip na full force cyberterrorism. Sa kabilang banda, ang mga state-sanctioned cyber groups tulad ng Cozy Bear, Fancy Bear, at SVR ng Russia ay nakatuon sa mga pangunahing supply chains ng kalaban pati na rin sa mga entity ng gobyerno at pribadong sektor sa labas ng supply chain upang makahanap ng mahalagang impormasyon at sensitibong data na maaaring gamitin bilang sandata.

The SolarWinds Hack of 2020

Sa unang bahagi ng Marso 2020, ang mga hacker mula sa Russia ay lumipas sa isang SolarWinds facility sa Texas. Ang pag-atake na ito, na kilala na bilang SolarWinds cyber-attack, ay nagbigay-daan sa mga hacker na mag-upload ng malware sa sistema ng kumpanya at ipuslit ang na-infected na code sa mga kompyuter ng kanilang mga biktima sa pamamagitan ng isang routine software update. Ang software system na ito, na tinatawag na Orion, ay isang kilalang programa na ginagamit ng maraming tao sa buong mundo ng information technology. Ayon sa isang ulat ng SEC, sinabi ni SolarWinds na may mga 33,000 active employees ang gumagamit ng Orion system. Gayunpaman, hindi naniniwala ang SolarWinds na lahat ng 33,000 empleyado ang nag-download ng na-infected na code at itinaas ang kalkulasyon ng kabuuang bilang ng na-infected na mga device na mga 18,000. Bagaman mas mababa ang bilang na ito kumpara sa 33,000 na empleyado na inilahad ng SolarWinds, ang mga na-infected na sistema ay patuloy na kinabibilangan ng mga major Fortune 500 companies, maraming mahahalagang entidad sa pribadong sektor, pati na rin ang ilang ahensya ng gobyerno.

Tulad ng lahat ng computer programs, kailangan ng Orion software ng routine updates upang manatiling ligtas at epektibo. Ginamit ng mga hacker ang impormasyon na ito upang pabagsakin ang proseso ng software development at isagawa ang kanilang atake. Sa pamamagitan ng pag-upload ng malware sa software ng SolarWinds at pagpapalaganap nito sa mga empleyado ng SolarWinds na gumagamit ng Orion system, nagawa

ng mga hacker na magtayo ng isang "backdoor" sa kompyuter ng sinumang nag-download at nakainstal sa software update na tila normal. Sa mga sumunod na buwan, libu-libong Orion users ang nag-dowload ng na-infected software.

Nang hindi inaasahan, nagkaroon ng access ang mga hacker sa kanilang sistema. Siyempre, naglabas ang SolarWinds ng karagdagang mga software updates pagkatapos ng initial na pag-atake, ngunit hindi nila alam na ang kanilang software ay napalitan na pala ng mga hacker sa unang lugar. Ito ay dahil sa unang breach, naglagay ng sistema ang mga hacker na mag-aalerto sa kanila tuwing ang SolarWinds ay magsisimula ng pagsusulat ng bagong software update. Karaniwan, kapag nagsusulat ng bagong software, gumagamit ng mas lumang bersyon bilang baseline. Sa kasong ito, ang baseline ay perceived na normal na mga linya ng code, at ito ang naging sanhi ng paniniwala ng development team ng SolarWinds na lahat ay maayos. Kapag handa na ang software para sa release, ang infected na code ng hacker ay nagsasabi sa sistema na palitan ang bersyon ng SolarWinds ng code sa kanilang halos magkapareho ngunit malisyosong code. Ang prosesong ito ay nagpapatuloy ng halos 9 na buwan at ganap na hindi natukoy ng SolarWinds.

Naging malinaw lamang ang atake nang ang FireEye, isang cybersecurity company mula sa California, ay nakilala na ang kanilang mga sistema ay compromised noong Disyembre 2020. Pagkatapos ng hindi mabilang na imbestigasyon ng SolarWinds at iba pa, natukoy na ang mga pag-atake ay naganap sa loob ng ilang buwan. Natuklasan din na ang mga hacker ay nakapasok sa mga sistema ng SolarWinds bago pa noong Oktubre 2019. Ang pag-atake na ito ay isang test run bago ang kanilang pangunahing atake noong Marso 2020.

Pagkatapos ng pagtuklas ng pag-atake, naglabas ng pahayag ang administrasyon ni Biden tungkol sa isang executive order na naglalagay ng ilang mga sanctions laban sa Russia. Bukod sa mga sanctions na ito, formal na inakusahan ng White House ang SVR ng Russia, na kinabibilangan ng mga grupo tulad ng APT 29, Cozy Bear, at ang Dukes, bilang responsable sa pag-atake na ito.

Departments and Operations Affected

Ang SolarWinds cyber-attack ay nakaapekto sa maraming tao mula sa karaniwang mga empleyado, hanggang sa mga mahahalagang dibisyon ng pribadong sektor, at maging sa ilang ahensya at departamento ng gobyerno. Ang mga naapektuhan ay kinabibilangan ng mga empleyado ng ilang kumpanya, partikular na ang SolarWinds, Microsoft, Cisco, Intel, Deloitte, pati na rin ang mga ahensya ng gobyerno tulad ng ilang bahagi ng Pentagon, Department of Homeland Security, State Department, Department of Energy, National Nuclear Security Administration, at Department of the Treasury.

Matapos matuklasan ang atake, ang Cybersecurity and Infrastructure Security Agency (CISA) ay naglabas ng isang ulat na nag-uutos sa lahat ng ahensya ng gobyerno na matukoy at masira ang lahat ng mga instance ng SolarWinds Orion software na tumatakbo sa kanilang mga network. Bagamat ang mga hacker ay nasa loob ng Orion software ng halos 9 na buwan bago pa man ang utos na ito, nagawa pa rin ng CISA na pigilan ang karagdagang pinsala.

May maraming kalituhan kung gaano kalalim ang naging epekto ng atake at kung anong impormasyon ang nakuha. Gayunpaman, ang pangunahing layunin ng atake ay espiya at pangangalap ng impormasyon, kaya't maaaring ipagpalagay na personal at sensitibong impormasyon ang nakuha. Bagamat maraming kumpanya at departamento ang nag-ulat ng mga tanda ng data breaches at malware, mahirap pa ring matukoy kung anong impormasyon ang nakuha at ninakaw, kung mayroon man.

Financial Fallout

Dahil sa malakihang pag-atake, ang pinansyal na epekto ay isang malaking alalahanin. Pagdating sa pinsala, pagkawala ng data at personal na impormasyon, at iba pang minor na epekto mula sa pag-atake, ang insurance lamang ay maaaring maging napakamahal. Ang iba pang pinansyal na alalahanin ay nakatuon sa pagtaas ng pondo upang makabuo ng mas magandang sistema ng seguridad at software, pati na rin ang pagpapabuti ng pagsasanay para sa mga empleyado. Bagama't ang mga empleyado ay hindi dapat sisihin sa buong pag-atake

na ito, ang pagkakaroon ng kaalaman kung ano ang gagawin kung mangyari muli ang ganitong sitwasyon ay napakahalaga, at ito ang dahilan kung bakit maraming kumpanya ang gumagastos ng malaking halaga ng pera sa mga pagsasanay at programa sa cybersecurity.

Bagama't hindi pa natutukoy ang lawak ng pag-atake, tinatayang ang kabuuang gastos ng paglilinis, kabilang ang mga gastos mula sa bawat apektadong entidad ng gobyerno pati na rin ang mga apektado sa pribadong sektor, ay nasa paligid ng $100 bilyon o higit pa. Ang SolarWinds ay gumastos ng humigit-kumulang $18 milyon hanggang $19 milyon sa unang tatlong buwan ng 2021 lamang sa pagsisiyasat ng breach. Hindi pa kasama dito ang gastos ng mga karagdagang panukalang seguridad at software, pagtaas ng pondo para sa mga bagong pagsasanay sa cyber para sa mga empleyado, at kabayaran para sa mga nakaramdam na lubos silang naapektuhan ng pag-atake na ito.

Future Security Concerns
Gaya ng nalalaman, malaking dami ng personal at sensitibong impormasyon ang nakuha sa SolarWinds cyber-attack. Malaking banta ito sa seguridad dahil madali lamang magamit ng mga hacker ang personal na impormasyon at access credentials mula sa pag-atake para makapasok sa iba pang bahagi ng supply chain ng Estados Unidos.

Isa pang alalahanin ay ang posibilidad na ilabas sa internet ang personal na impormasyon ng mga mamamayan ng Estados Unidos, militar, at mga opisyal ng gobyerno. Kapag nasa internet na ito, madaling maa-access ng mga kaaway ng Amerika at maaaring magdulot ng matinding pinsala sa publiko

Conclusion
Sa kabuuan, ang SolarWinds cyber-attack ay isa sa pinakamalaking cyber-attacks laban sa Estados Unidos sa mga nakaraang taon. Hindi lamang mararamdaman ang mga epekto ng pag-atake na ito sa mga darating na taon mula sa unang pagtuklas, ngunit magbabago rin nang malaki ang kaligtasan ng Estados Unidos at ng cyberspace sa kabuuan.

Maraming nakuha ang Russia mula sa pag-atake na ito kabilang ang mahalagang intelihensiya tungkol sa supply chain ng Estados Unidos. Bagamat mabigat ang naging tugon ng Estados Unidos laban sa Russia para sa pag-atake na ito, maaaring ipagpalagay na magpapatuloy ang Russia sa kanilang mga pag-atake sa Estados Unidos. Ang Russia ay umuunlad sa pamamagitan ng pagsakal sa ekonomiya ng isang bansa at ang karagdagang impormasyon mula sa pag-atake na ito ay tiyak na makakatulong sa kanila.

Sa mas malawak na pananaw, bagamat maaaring hindi nagdulot ng malaking pinsala ang Russia sa imprastruktura ng Estados Unidos, nagawa pa rin nilang sirain ang tiwala ng maraming tao sa seguridad ng Estados Unidos. Maraming tao ang naniniwala na hindi mapapasok ang Estados Unidos mula sa mga banta mula sa labas ng mundo. Gayunpaman, tulad ng nakikita sa mga epekto ng SolarWinds attack, hindi ito ang kaso. Ang SolarWinds ay dapat maging isang malaking wake up call para sa mga malalaking korporasyon at ahensya ng gobyerno. Ang mga banta ng cyber world ay hindi dapat binabalewala. Bagamat mukhang maliit, kahit ang pinakamaliit na cyber events ay maaaring maging pinakamalaking banta sa pambansang seguridad.